CLAIMS

I claim:

1. A method comprising:

using a biometric generator to obtain a biometric signature of an individual;

bonding the biometric signature to a data storage device;

requiring the biometric signature of the individual to access a data record stored on the data storage device;

controlling an access to the data storage device by using a data console, the data console being a secure input/output device;

maintaining a credibility record associated with the data record;

using a metadata query to request a disclosure of the data record; and

allowing the individual to control the disclosure of the data record.

2. The method of claim 1 further comprising:

generating an encryption key based on the biometric signature of the individual; and

using the encryption key to encrypt the data record.

3. The method of claim 1 further comprising:

obtaining the biometric signature of a session operator, the session operator operating the biometric generator; and

recording a session history in the credibility record.

4. The method of claim 3 wherein the session history comprises:

a unique identifier of the biometric generator;

the biometric signature of the session operator; and

a session time.

5. The method of claim 3 further comprising preventing the session operator from operating the biometric generator when the biometric signature of the session operator does not match the biometric signature of an authorized operator.

6. The method of claim 1 further comprising:

obtaining the biometric signature of a console operator, the console operator being a person operating the data console; and

recording an access history in the credibility record.

7. The method of claim 6 wherein the access history comprises:

an unique identifier of the data console;

the biometric signature of the console operator;

an access type; and

an access time.

8. The method of claim 6 further comprising:

requiring the console operator to enter an authorization code prior to allowing the console operator to access the data record;

preventing the console operator from accessing the data record when the console operator does not enter a proper authorization code; and

storing the authorization code in the credibility record.

9. The method of claim 1 wherein using a metadata query further comprises:

evaluating of the data record without disclosing the data record to a querying party; and

evaluating of the data record without disclosing the metadata query to the individual.

10. The method of claim 1 wherein allowing the individual to control the disclosure of the data record further comprises:

allowing the individual to deny a specific data query;

allowing the individual to deny the metadata query;

allowing the individual to authorize the disclosure of the data record; and

allowing the individual to authorize a partial disclosure of the data record.

11. The method of claim 1 further comprising recording a query history in the credibility record.

12. The method of claim 11 wherein the query history comprises:

a data query authorization code;

an identification of the querying party;

the unique identifier of the data console;

the biometric signature of the console operator; and

a query time.

13. The method of claim 1 further comprising:

assigning a credibility factor to the data record based on an evaluation of the credibility record;

changing the credibility factor when an element in the credibility record is compromised; and

sending a broadcast notice associated with a change in the credibility factor.

14. An apparatus for private information access rights management comprising:

a biometric generator to analyze a unique biological characteristic of an individual and to generate a biometric signature for the individual wherein the biometric signature is reliably replicable;

a data storage device to store a data record wherein the data record belongs to the individual and the data storage device is locked by the biometric signature; and

a data console to control an access to the data record wherein the data console is a secure data input/output device and the access comprises one of a data query and a data entry.

15. The apparatus of claim 14 further comprising a generator authorization procedure.

16. The apparatus of claim 15 further comprising a generator operator biometric signature match.

17. The apparatus of claim 14 further comprising a data console authorization procedure.

18. The apparatus of claim 17 further comprising an authorization code.

19. The apparatus of claim 14 further comprising an authorization to disclose the data record wherein the individual controls the authorization to disclose the data record.

20. The apparatus of claim 14 further comprising a credibility record associated with the data record.

21. The apparatus of claim 20 wherein the credibility record comprises a session credibility factor.

22. The apparatus of claim 20 wherein the credibility record comprises a biometric operator credibility factor.

23. The apparatus of claim 20 wherein the credibility record comprises an access credibility factor.

24. The apparatus of claim 20 wherein the credibility record comprises a data console operator credibility factor.

25. An article of manufacture comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

generate a biometric signature of an individual;

bond the biometric signature to a data storage device;

require the biometric signature of the individual to access a data record stored on the data storage device;

control an access to the data storage device by a data console, wherein the data console is a secure input/output device;

maintain a credibility record associated with the data record;

use a metadata query to request a disclosure of the data record; and

allow the individual to control the disclosure of the data record.

26. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

generate an encryption key based on the biometric signature of the individual; and

use the encryption key to encrypt the data record.

27. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

generate the biometric signature of a session operator, wherein the session operator operates the biometric generator; and

record a session history in the credibility record.

28. The content of the machine-accessible medium of the article of manufacture of claim 27 wherein the session history comprises:

a unique identifier of the biometric generator;

the biometric signature of the session operator; and

a session time.

29. The article of manufacture of claim 27 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to prevent an operation of the biometric generator by the session operator when the biometric signature of the session operator does not match the biometric signature of an authorized operator.

30. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

generate the biometric signature of a console operator, wherein the console operator operates the data console; and

record an access history in the credibility record.

31. The content of the machine-accessible medium of the article of manufacture of claim 30 wherein the access history comprises:

an unique identifier of the data console;

the biometric signature of the console operator;

an access type; and

an access time.

32. The article of manufacture of claim 30 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

require the console operator to enter an authorization code to access the data record;

prevent an access of the data record when the console operator does not enter a proper authorization code; and

store the authorization code in the credibility record.

33. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

perform an evaluation the data record wherein the data record is not disclosed to a querying party; and

perform an evaluation of the data record wherein the metadata query is not disclosed to the individual.

34. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

allow the individual to deny a specific data query;

allow the individual to deny the metadata query;

allow the individual to authorize the disclosure of the data record; and

allow the individual to authorize a partial disclosure of the data record.

35. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to record a query history in the credibility record.

36. The content of the machine-accessible medium of the article of manufacture of claim 35 wherein the query history comprises:

a data query authorization code;

an identification of the querying party;

the unique identifier of the data console;

the biometric signature of the console operator; and

a query time.

37. The article of manufacture of claim 25 further comprising:

a machine-accessible medium including content that, when accessed by a machine, causes the machine to:

assign a credibility factor to the data record based on an evaluation of the credibility record;

change the credibility factor when an element in the credibility record is compromised; and

send a broadcast notice associated with a change in the credibility factor.